Macomb/St.Clair Workforce Development Bd., Inc.

IT Information Security Policy

User Review & Acknowledgment signature page Instructions

Please carefully review all binding provisions contained herein and once you clearly understand the terms and conditions of use and support responsibilities of all parties and can agree to work within them as presented please complete all sections of the Acknowledgment Page (page 12) and then sign and return the original to Allen H. West; IT Administrator, Macomb/St. Clair Workforce Development Board, Inc.
For questions/clarification contact Allen West via email west@macomb-stclairworks.org or 1) Phone 469-5272, 2) Fax 469-7488 *Thank you!*

Table of Contents

The topics covered in this document include:	PAGE
a. Overview	2
1. Introduction & Purpose	2
2. Policy Violations & Disciplinary Rights	2
3. Administration of Policy Provisions	2
b. Statement of User Responsibility – (Goals of Proactive Compliance Services/Support)	3
1. Managers and Supervisors	3
2. Staff; Subcontractors, MI Works! Customer Users	3
3. IT Administrator	4
4. IT Technician Support Services	5
C. Internet, E-mail, and other related Network Services "Use Privileges"	5
1. Policy Provisions	5
2. Acceptable Use	6
3. Unacceptable Use	6
4. Downloads: Upgrades, Demo's, Patches, Drivers, Freeware/Shareware & BETA Systems	6
5. IT Monitoring & Client/Server Audits of Use & Productivity	7
d. Subcontractor IT Equipment & "Use/Support" (3rd party support limitations-added 7/17/2002)	7
1. IT Support Services to Subcontractors/Co-located Staff	7
2. Warranty/Licensing Restrictions for 3rd party IT Equipment (Affecting ability to Help!)	7
e. Computer Viruses Background – Prevention Techniques	8
1. IT Virus Prevention Responsibilities	8
2. Staff/Subcontractor/ Customer Use - Virus Prevention Responsibilities	8
F. Secure Access - Login Codes & Password Settings	8
1. Network Security Maintenance & Modifications - IT responsibilities	9
2. User Security Responsibilities for Staff and Subcontractors	9
3. Supervisory Personnel Responsibility – Timely Notice of Changes	9
4. Human Resources Type Changes – Name Changes, transfers, terminations.	9
G. Confidential Information Security – Protecting Privileged Privacy Data	9
H. Physical Security & Redundant Backup Plans for IT Equipment/Services Support	9
1. IT Administrator Responsibility in Development and Implementation – Multiple Redundancy	9
2. Staff & Subcontractor User Responsibilities.	10
3. Supervision of Users – Assurance of Mission Related Use & Accountability	10
I. Copyrights and License agreements	11
1. Legal Reference	11
2. Scope of Coverage	11
3. IT Responsibilities Re: Copyrights/Licenses	11
4. Staff and Subcontractor User Responsibilities Re: Copyrights/Licenses	11
5. Civil Penalty Violations	11
6. Criminal Penalty Violations	11
Acknowledgement of IT Information Security Policy – Review/Affirm Signature Page	12

Developed and authored for Macomb/St. Clair Workforce Development Board, Inc. by Allen West; Purchasing/PC Tech/Network & Website Administrator .
With review, consultation, and authorization of John H. Bierbusse; Executive Director for Macomb/St. Clair Workforce Development Board, Inc.

Macomb/St.Clair Workforce Development Bd., Inc.

IT Information Security Policy

A. Overview

The enclosed policies and directives have been established in order to:

- **Protect our investment in the enhancement of the delivery of services to MI Works! Customers.**
- **Improve productivity of staff through efficient and timely serviced network tools and resources.**
- **Safeguard the information contained within these systems-maintaining Privacy and Confidentiality.**
- **Educate all users of the IT Services in a proactive manner to improve services and reduce/prevent problems.**
- **Reduce business and legal risks and protect the good name/reputation/mission of the Board.**

1) Introduction & Purpose - IT Security Policy

The Computer information systems and networks are an integral part of business at Macomb/St. Clair Workforce Development Board, Inc. The Board has made a substantial investment in human and financial resources from available grants to create these systems for staff, customers, and subcontractor partners so as to develop a comprehensive system of services delivery and a customer friendly environment to maximize potential of all users.

2) Policy Violations & Disciplinary Rights

The Board's intent is to work in Good Faith and Proactive with all Subcontractor Entities and their respective employee's and is committed to provide a Quality IT System Structure of Equipment, Support and Maintenance so as to accomplish the Goals of the Contract for the benefit of all concerned.

The IT Services Network has become an integral part of maximizing and enhancing services to our Primary Target Goal "The Customer" (as defined in our various Grants and Acts of Congress) and to improve the productivity of the users and staff. Working outside the Policies places our Mission in jeopardy and shortchanges "The Customer" and coworkers. It is our desire to work together with all Users bound by these procedures through ongoing information, education and explanations as to why some of these areas are required so as to create a mutual understanding. We believe the better informed and educated the users are, the fewer problems we're likely to encounter and more likely to work as a **TEAM**.

Where there is a failure to observe these guidelines, and any related attachments, email/fax notification updates and intermittent notices from the Board related to IT Policies may result in the Board's pursuit of immediate corrective action that may include disciplinary measures**.** The Board's recourse will depend upon the type and severity of the violation; whether it causes any liability or loss to the Board, and/or the presence of any repeated violation(s) or where user(s) actions demonstrate choices contrary to and that ignore instructions from IT Staff or the policies contained herein or an unwillingness to work together to correct the issue. Such actions would warrant the termination of User privileges on the Board's Network and would be blocked from all IT Services immediately pending resolution.

Realizing that most "Users" of the Board's IT System are subcontract employee's we will work with Subcontractor to resolve disputes in seeking corrective action and remediation. While it is not the Board's policy to interfere with a Subcontractors Labor Management Human Resource Policies and their Staff, it reserves the right under the Subcontract to request disciplinary actions that may include termination of the affected individuals as it relates to said contract and the right to seek recovery of compensation for any resulting IT damages the Board may have incurred.

It is understood and agreed herein that the use of the Internet and the Board's IT Services is a Privilege and not a right, and inappropriate use can result in immediate cancellation of those privileges and may result in discipline.
We reserve the right to remove and/or disable the "User" Network and Client IT Services/Equipment from active use immediately pending corrective action or where said violations threaten to damage equipment or violate the Security of the Board's IT LAN/WAN System and the integrity of Customer Data and pose a risk of damage to the Board's equipment. Each employee is responsible for using good judgment when using or supervising the use of the Board's Internet Services and all related Network Services/Equipment by the "Public Customer" that it supervises.

3) Administration of Policy Provisions

The Information Technology Unit of the Board is responsible for the administration of this policy through consultation and approval/support and direction with the **Board Executive Director; John Bierbusse** and based upon Industry Standards/Practices and provisions contained herein and any/all appendix/attachments related email updates and MDCD and Grant Policies governing our programs.

- **Allen West; Purchasing/PC Tech/IT & Website Administrator** west@macomb-stclairworks.org
- **Allan Eisenhauer; PC Technician/IT Services Assistant** allan@macomb-stclairworks.org

B. Statement of User Responsibility (Goals of Proactive Compliance Services/Support)

General responsibilities pertaining to this policy are set forth in this section. However, it should be understood that the IT System Technology changes so rapidly that not every identifiable situation could be planned and provided herein and it is expected that users exercise reasonable care when using these services/equipment and when in doubt consult with IT Administrator.

1) Managers and Supervisors must:

- **Inform Staff -** ensure that all appropriate personnel are aware of and comply with these policies and any subsequent update notices from IT Administrator.
- **Create appropriate performance standards**, **control practices, and procedures** designed to provide reasonable assurance that all staff and subcontractor users observe this policy.
- **Establish On-site Security Measures** that provides proper supervision/accountability of Public PC's to prevent inappropriate stealth and anonymous use or abuse. Such use can cause damage to our Network and others or be used to communicate with inappropriate groups not related to our mission at-hand and pose a risk to "National/Homeland Security". In retrospect, investigations after 9/11 showed that the terrorist cells used Public PC's to communicate with one another around the country so as to disguise their plans in stealth and anonymous modes. Local staff needs to be cognizant of this and observe the Customer use and make sure that we have traceable and verifiable ID back to whom the user was. A log of User's with verifiable ID checks MUST be used to prevent Stealth/Anonymous use.

- **Observe and Identify skilled PC users on staff and encourage local mentoring "Self Help**" in the use of their day-to-day programs. Enhancing mission related objectives and maximizing staff resources. This is as it relates to things like common printer maintenance and jams as addressed in one's Printer User Manual.
(This provision does not extend to or expect users to attempt IT repair services.)

- **Coordinate User Specialty Applications Training** - While IT may install, configure and troubleshoot specialty program applications like "Open Options" "PLATO", "MOIS" and others and monitor these services, it would be rare that IT would be a full-time user of these services and cannot be expected to be a trainer in those programs usage in most cases. IT Staff is constantly in a State of Training in their Technical areas and simply cannot have time to study these areas also when they are not "Users" of those services. That's why it's important to identify the highly skilled staff or subcontractor training specialists or have experienced users to mentor and train new people or enhance existing staff that may lack an understanding and bring them up to par. IT sets the stage for use of the Specialty Applications but cannot be expected to serve as a Knowledgebase Helpdesk Resource for such internal program components.

2) Staff; Subcontractors, MI Works! Customer Users Shall:

- **Submit "IT Work Requests" in writing via Email to IT Administrator** (fax only when email is not available) and are required to provide the equipment 1) Property Tag Numbers or Serial Number to reference the inventory database for identifying components makeup, age, Vendor contacts and existing warranty status. 2) A description of SYMPTOMS is vital so as to enable a problematic diagnosis prior to scheduling services/support. "Not working" statements fails to identify any symptoms. An example would be taking one's auto in for repairs and telling the Auto Tech it's not working won't help get your car repaired or going to the doctor and saying I'm feeling ill but not describing the symptoms would prevent the Doctor from being able to assist. Incomplete work requests simply create unnecessary extra email and wasted time to ask for more specific info and only serves to delay support since Incompletes won't be assigned support.

- **Understand Verbal Work Requests are prohibited**. **"**Avoid Verbal Orders (AVO) "an old business standard which applies here. Verbal requests are not acceptable since they fail to meet standard business practices of accountability of services delivery and a history of IT activity/support. This is just a common business practice and a required standard of the IT Industry yet many staff come to expect support to be delivered without having to provide the most basic info so as to **"HELP US HELP YOU"** The Support system has been developed to keep the work request required content to a minimum and only asking for a very brief informal summary and it has been designed to be as short and convenient as possible since we're aware of the volumes of paperwork common to your daily work. In comparison with the Macomb County MIS forms, they have a full two-page document that must be completed for each work request that must go through a multitude of people for review and approval and then assignment. I can't make our system much easier or streamlined than it is without comprising our basic responsibilities. Even where Emergency Verbal requests may take place when the situation warrants, that user will be responsible for providing notice in writing as soon as possible after the event for Task Management Records, History, and accountability of IT Services delivered.

- **Ensure that communications are for professional reasons** that do not interfere with one's productivity.

- **Be responsible for the content of all text, audio, or images that (s)he places or sends over the Internet**. All communications MUST have the staff and subcontractor user's name attached.

- **Not copy or transmit copyrighted materials without permission and assume all web content to be protected**.

IT Information Security Policy

- **Know and abide by all applicable MSCWDB security and confidentiality policies**.
- **Run a virus scan on any executable file(s**) and do not open email attachments from unknown sources.
- **Avoid transmission of nonpublic customer information and abide by Confidentiality standards**.

- **Regularly clean external areas to prevent dust/dirt and any moisture accumulation on IT Equipment** – The Board will supply expendable materials specifically designed for cleaning IT related equipment for user self-maintenance of the work area just as one does for other work area items like phones, calculators and desk components. General cleaning of Peripheral devices, i.e.; keyboards, mouse, printers, monitor using cleaning wipes, sprays, and air cans, swabs, etc. **Cleaning of these external work area components is NOT an IT Technician's Responsibility.**

- **Provide Reasonable Care & Use of IT Equipment** - The Board has invested significant financial and human resources as a primary tool in delivering services to the Customer and must be used with care to prevent damage. Never force connections that don't seem to meet or pull on loose cables since pin/connector and network jack damage is likely to result disabling one's system or making the item unusable and will not be covered by the Vendor Warranty.

3) IT Administrator Is Responsible for and Shall . . .

Develop and maintain written standards and procedures *(contained herein and interim updates)* necessary to ensure implementation of and compliance with these policy directives and to educate and inform its "Users" to prevent non-compliance and enhance "User" competencies, Productivity and minimize User downtime.

- **Coordinate all IT Work Requests.** Receives, and studies all Work Requests to determine Problematic Diagnosis from symptoms presented, the level of priority according to the Mission at-hand via Triage System, the history of the equipment, remaining warranty coverage's and the possibility of having to acquire replacement components through budget funds. Estimates resulting downtime and identifies alternate redundant services when available pending receipt of replacement parts and repairs. Delegation of Task to the IT Technician or Vendor Engineer. .

- **Design and publish updates and postings to the Board's Website and it's Growth.**

- **Provide appropriate support and guidance to assist staff and subcontractor users to fulfill their responsibilities** under this directive as well as Plan and Direct the IT Technician to Monitor/Audit IT License compliance and Inventory updates.

- **Track Services Usage and issue reports to the Board, Executive Director and local Supervisors.**

- **Test & Monitor all Server Systems and Telecom T1 lines for trouble events throughout the Workday.** Coordinate Engineering Tasks to minimize downtime and smooth delivery of services through the Network and track/report inappropriate use of services on the network. At this point there are 9 Servers and 5 T1 lines that require full-time monitoring to pinpoint failures as soon as possible to investigate and coordinate return to normal services to minimize downtime for User staff and it's Customers.
- **Conduct ongoing review of Network Design Topology and Services** and identify areas of improvement and growth of the network to the benefit of the Boards Mission and MI Works Customers and Redundancy Plans.
- **Coordinate Purchasing of Goods and Services and using Competitive Bids –** Under the Board's structure the IT Administrator is also the Purchasing Officer establishing systems that provide goods and services in accordance with State and Federal Procurement Guidelines and the Boards Grants and via competitive bids to maximize the financial resources of the board in it's delivery of services to it's Customers. Procurements include everything from monthly expendable/perishables to furniture; copiers, faxes and IT related equipment and software.

This provision is contained herein because it is rare that the IT Administrator is also the Purchasing Officer. While possessing this combination serves to benefit the IT System overall and the Purchasing and IT Budgets are maximized through this combination it's important to understand that there are times when available workday must be split to meet the responsibilities of the Purchasing area also and thus requests are being served from users in both areas from all the subcontractors and Board Office that are time intensive. So not only are decisions made on Triage with IT but decisions on also servicing your equipment and supply needs and processing Vendor invoice payments with Accounting, and Inventory Database updates have to also be addressed at the same time. This is one of the reasons that incomplete Work Requests can be extremely frustrating, these incompletes necessitate repeat wasteful emails to obtain the most basic correct information required under this policy. Simply isn't even time available in the day to waste it in such a manner and only serves to delay the Services to assist the User and others waiting, making sure requests are properly submitted will expedite assigning the Help you need and preplan what troubleshooting may be required and enable meeting the Purchasing needs of your offices also in a timely manner. Everyone benefits as a result.

- **Ongoing In-Service Training via CBT, Classroom, Books, and Distance Learning** for Network Support in the Delivery of IT Services in the MI Works Customer Centers so as to enhance and keep IT competency skills as current as possible with the needs of the Board's network LAN/WAN equipment.

4) IT Technician Support Services Responsibilities include

Work Requests are forwarded through the IT Administrator for delegation to the IT Technician according to established "Triage" mission related priorities that have been utilized for the past 5 years for accountability and reference of support history of problem solving events.

- Troubleshooting events forwarded by the IT Administrator with the user's system to resolve the issue with the user and the Vendor if required in accordance with IT Triage scheduling and as delegated by the IT Administrator.
- Requiring users to submit Work Requests in writing so as to enable an event history and accountability of tasks performed. Documentation of IT tasks is paramount and a foundation of A+ Technical Training and Support Programs.
- Coordinating Warranty replacements via phone Troubleshooting with Vendor and notifies IT Admin for Inventory updates and any RMA processing and shipping return to manufacturer.
- Responding to User IT System component failures to diagnose and repair systems back to normal operational status.
- Performing onsite configurations of new IT equipment and coaches Users in its use.
- Installations, upgrades, patches, drivers and new authorized/licensed software applications to user systems.
- Monitors and Audits License Status of application programs on each user PC system and is directed to printout audit log's to support compliance status of PC's and also to remove immediately and report any unlicensed software found.
- Repairing and replacement of peripherals, devices, and components of workstations and printers. i.e.; motherboards, RAM, printers, CD ROMs, Hard Drives, NIC's, Monitors, mouse, keyboard, video cards and network cable, etc..
- Runs small network cable projects (small scale of < 10) where more cost effective versus Engineering Contractor.
- Establishes redundant resources for local users in case of default printing device fails they have a backup resource.
- Rotates local Server Backup Tapes weekly for off-site storage in case a catastrophic event at any center.
- Participates in ongoing In-Service Training for User Support in the Delivery of IT Services in the MI Works Customer Centers so as to enhance and keep IT competency skills as current as possible with the needs of the Board's equipment.
- Work with local users as a partner and coach, educating them on proper use and prevention of recurring problems.
- Documents Work Request History into a database for baseline reference points for future events & reports.
- Reports any/all abuses directly observed or have knowledge of from other sources back to the IT Administrator.
- Retrieving some IT systems for Bench Repair at the Board Office when more time and cost efficient to do so.

C. Internet, E-mail, & related Network Services Use Privileges

The Internet is a very large, publicly accessible network that has millions of connected users and organizations worldwide. One popular feature of the Internet is email; the Board has chosen **"Microsoft Exchange Server "Outlook"** as its default Client Use and Remote SMTP Web Based Email Messaging Services. The Board has provided High Speed Dedicated and Point-to-Point T1 Lines between all Centers to the Server Hubs/Switches/Cache Engine with state of the art Security Firewall so as to provide the most efficient secure means of connectivity for it's subcontractors, staff and MI Works! Customers.

"Staff; subcontractor users and MI Works Customers are responsible for ensuring that the Internet and Email is used in an effective, ethical, productive, lawful and professional manner." . . .

per John Bierbusse; Executive Director, Macomb/St. Clair Workforce Development Board.

1) Policy Provisions

- Access to the Internet is provided to Board staff, subcontractor users and Customers for the purpose of delivery of planned program services and goals as approved by the MI Dept of Career Development for its customers. Staff and subcontractor users are able to connect to a variety of government, educational, non-profit and business related information resources around the world with a virtual limitless library of informational resources. It is our Goal to maximize and expedite the availability and use of said services to the benefit of all.
- Conversely, the Internet is also replete with risks and inappropriate material. The Board has chosen "Websense" Internet Filtering as its tool to prevent such access by blocking access to inappropriate sites. We may also create custom filters to block websites that may not be on the database or selectively add/remove filters.

These Policies have been developed to ensure that all staff and subcontractor users and customers are responsible and productive Internet users and to protect the Board's interests and the mission related services to its Customers.

2) Acceptable Use

Staff and subcontractor users and customers using the Internet are representing the Board.
Some Examples of acceptable use are (certainly not all-inclusive):

- Using Web browsers to obtain business/mission related info from commercial Web sites.
- Accessing job-related, career oriented training activities, and support services databases for information.
- Using e-mail for the Board's business and mission as well as maintaining customer liaison contacts.
- Using PC's to receive or deliver training, tutoring services, and develop and print resumes/cover letters, etc.

3) Unacceptable Use

Staff and subcontractor users must not use the Internet for purposes that are illegal, unethical, harmful to the Board, or nonproductive. **Some Examples of unacceptable use are (certainly not all-inclusive):**

- Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others as well as any pyramid schemes or multilevel marketing initiative (these are considered a private business venture initiatives). Chain e-mail is used for planting viruses, to commit misrepresentation/fraud, and it hogs vital server resources.
- E-mail broadcasting of Spam or Mail Flooding; i.e., sending the same message to more than 10 recipients or more than one distribution list outside the Boards Exchange Server "Outlook" Email Workgroup System for the purpose of spamming or mail flooding, this action can interfere with and disable the recipients Email system and hog system resources at both ends.
- Third Party Instant Messaging (IM) & Chat Services is prohibited until our Network Engineer Consultants determine it can be safely incorporated through our Firewall without jeopardizing the integrity/efficiency/security of our Network.
- Conducting a personal business venture(s) using Board resources.
- Transmitting any content that is offensive, harassing, fraudulent, expressing political ideologies/support, advocacy group
- Solicitation of money for services outside the scope of the Boards Mission without Board's Executive Director's review and authorization first is prohibited. Staff related functions that require contributions, like luncheons, casual day, holidays, and interpersonal exchanges that promote +morale and unity of mission and where participation is voluntary is acceptable. Solicitation of Charity donations should be reviewed and approved through the Executive Director since the Board has participated in many sanctioned fund raising events including United Way and many others. Solicitation of funds for Political Parties, Candidates and/or Causes is strictly prohibited by "Hatch Act" see Memorandum from Dr. Barbara Bolin Director of MI Dept of Career Development and website link. http://www.michigan.gov/mdcd/0,1607,7-122-1683-44342--,00.html
- Playing Multimedia Games of any kind that may be resident or installed as third party software or via CD by the user or available for playing from one's browser on-line during one's paid time. Primary example would be Solitaire or other on-line gaming systems and download services that have been determined to violate Copyright Laws, i.e.: Napster.

On-line Gaming Services (Gambling) and Network Game playing is strictly prohibited at all times.

4) Downloads: Upgrades, Demo's, Patches, Drivers, Freeware/Shareware& BETA

- An example of an authorized download would be Adobe Acrobat "Reader", which is "Freeware" and compatible with our existing work station/server Operating Systems, and Internet Browsers and used within the Boards Website for on-line document referencing, Minutes posting, Catalog of Services, and printing of forms via PDF.
- In general, File downloads from the Internet are **not** permitted unless said download has been pre-approved and tested through the IT Staff of the Board and then authorized as mission related and compatible with existing IT devices and OS.
- Staff and subcontractor users are prohibited from downloading patches or upgrades to their operating systems or browsers on their own because of conflicts that may disable such systems that would require extensive technical support to correct as well as the loss of use of one's system pending service and potential loss of all said employee's working/customer files as a result and prevent user ability to carry out their job responsibilities.
- Absolutely NO BETA Test Downloads or unlicensed Shareware/Freeware or Commercial Demo's are to be used. BETA means it's in the process of being tested and not ready for market and you're the guinea pig and the Board doesn't want to use it's system in such a manner. Commercial Demo's can conflict with existing resources on one's PC. The Board welcomes the review and consideration of software enhancements that can be tried and tested first by IT staff. Another reason is to maximize budget resources because it may be a program that's useful throughout the Network or other areas and significant license fee reductions can take place with Volume Licensing that can equal a significant amount of money.

Precautionary Note! Bringing in third party unlicensed/unauthorized software or time trial programs contrary to warnings herein and then deleting with the thought a software audit won't identify it simply is a false assumption.. Our Audit software identifies all installations even those one may think was removed. – (IT Admin)

5) IT Monitoring & Client/Server Systems - Audits of Use & Productivity

- All messages created, sent, or retrieved over the Internet (with the exception of confidential data sources protected by Privacy Laws and Program guidelines) are the property of the Board and may be regarded as public information. Macomb/St. Clair Workforce Development Board, Inc. reserves the right to access the contents of any messages sent over its NETWORK if the Board believes, in its sole judgment, that it has a business need to do so to examine compliance, productivity and acceptable use.

- "Websense" Security Filters and Monitoring System are installed on a full-time Server. This subscription service database is updated each night via the Internet as a preventative measure to keep filters updated and BLOCK unauthorized/inappropriate websites and prevent unacceptable use by the public and staff users. These database filters are updated nightly and are customizable to meet local needs/restrictions. Should a filter block a "Mission Related" site the filter can be adjusted with justification notice to IT Administrator and a custom filter would be established to include it's use following review/testing and approval. This software also tracks and reports the productivity of all systems, charting by category by all user PC's and categories, this service will be enabled within the next 3-6 months as it requires a separate database server to chart and report the log activity.

- All communications, including text and images, can be reviewed by IT Network Administrator and with approval of Board Director disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. One must think in terms of our system being a huge Bulletin Board and have an understanding that if you weren't willing to post your ideas, comments and feelings for everyone to see (including gossip, or damaging and inappropriate comments about coworkers or management) then keep it private because they could end up on that so called bulletin board and have serious consequences. It is not our intent to censor one's thoughts but common sense should prevail and keep it private, using email to use profanity, rumor/gossip and personal attacks against others (including one's management staff) creates a record of proof against oneself that could lead to serious consequences of self incrimination. This simply means don't put anything into your e-mail messages that you wouldn't want to see on the front page of the newspaper or the Bulletin Board scenario where it could be seen by coworkers and management.

  This area is being emphasized since several incidents have actually occurred during the past 18 months that has resulted in serious consequences, Leading to the dismissal of a subcontractor Employee and a few others that have ignored these warnings only to become victims in the process, exposing themselves to disciplinary action by their employer.
  The Board IT initiates a review where allegations have been presented that represent possible violation(s) of the policies herein to determine the scope and degree and whether the allegations can be confirmed by an IT Review to protect the integrity and professionalism of the Board's system and prevent further violations and possible damage and seek appropriate corrective actions. Subcontractors may also pursue their own review in accordance with their applicable Labor Management Policies and request copies of any support documents from the Board's user system by submitting a request in writing to the Attention of our Executive Director for review and approval.

- All Privacy Act and Confidentiality Data remains protected as governed by state and federal statute. It has not been the practice of the Board IT Network Administrator to infringe upon and review user messages on user PC's or the Email Server without cause. In practice, we prefer to work proactively and from a position of Trust with those within the Network, however, where a breach of policy contained herein or Security log's are observed or violations are reported we reserve the right to examine and investigate those areas of the Network to ensure compliance and protect the integrity of the Network Services and the Mission of the Board and prevent harm to the system and other users. Most Courts have upheld this right.

D. Subcontractor Vested IT Equipment "Use & Support it"

Any Subcontractor or co-located staff using foreign IT Equipment yet connected to and using our Network Services is still expected to abide by these policies in addition to those of their own organization whenever possible.

1) IT Support Services to Subcontractors/Co-located Staff

(For Support timelines see IT Triage Helpdesk Document Handout will be posted on IT Helpdesk WebPage in the near future.)

- Our goal is to expedite support so as to return IT Services to normal as quickly as possible and prevent delays in waiting for the support to come from the State Service Provider despite the fact the equipment is not ours. Where IT work request events are caused by **foreign program applications** that we lack training to support and the event is conflicting with our IT System we reserve the right to either refuse support to the event and require the Agency request support from their Agency, or we may offer to remove the application program that's conflicting if deemed as an unnecessary so as to prevent repeated support calls and downtime.

2) Warranty/Licensing Restrictions for 3rd party IT Equipment

- We hold no Warranty Support rights to Subcontractor procured and vested equipment and thus should hardware failures occur that require Warranty Support by the OEM Vendor and we hold no Licensing Rights or ownership vesting, then it must be the responsibility of the Subcontractor/Co-located Agency to resolve such issues. Nor do we provide Board budget funds to replace parts on IT equipment that isn't property of the Board unless preauthorized by the Board Executive Director.

E. Computer Viruses Background - Prevention Techniques

Computer viruses are programs designed to make unauthorized changes to programs and data. Therefore, viruses can cause destruction of board resources. It is important to know that:

- Computer viruses are much easier to prevent than to cure. **Preventive Measures are Priority #1**

- Defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, maintaining virus-scanning software, and avoiding the transfer of files via floppy disk. **The use of floppy disks should be avoided whenever possible.** All working files should be processed from one's hard drive or through primary network services. Floppies are intended as a "secondary storage" not as one's primary storage and floppies make the network vulnerable to virus contamination if the user lacks an up to date anti-virus package on one's PC at home or other institution. The Board has no way of knowing whether the floppy has been used in an external system that may lack virus detection with current signature files and since the type of viruses change daily and can hibernate for long periods of time undiscovered until it's triggered to execute - this makes our entire network vulnerable to damage.

1) IT Department - Virus Prevention Responsibilities

(Norton *Enterprise Edition Anti-Virus is on all Server Network Access Points)

- Install and maintain appropriate anti-virus software on the network. Local users are protected via *Norton Enterprise and the Security Firewall. Norton is programmed with after hours live updates weekly and the logs on all Servers are also viewed weekly **unless** an Alert has been received from Symantec Norton Anti-Virus. Alerts require immediate review of logs and interim Live Updates via the Web when Alert's are received for capture, quarantine or deletion and follow the recommendations of Symantec to prevent exposure and contamination of the Boards Network.

- Respond to all virus attacks, resolve to quarantine, clean, destroy any virus detected, and document each incident.

2) Staff/Subcontractor/ Customer Use Virus Prevention Responsibilities

- Staff and subcontractor users shall not knowingly introduce a computer virus into Board computers.

- Staff and subcontractor users **shall not load diskettes of unknown origin**. **Floppy use should be avoided**.

- Incoming **authorized diskettes** shall be scanned for viruses with **Up-to-date Anti-virus before they are read**.

Any associate who suspects that his/her workstation has been infected by a virus shall **IMMEDIATELY POWER OFF** the workstation and call/fax/ or email the IT Administrator and use alternative resources until the PC has been scanned, diagnosed, cleaned and authorized for reactivated use by IT Staff. **Never open attachments from unverifiable sources.**

F. Secure Access - Login Codes & Password Settings

The confidentiality and integrity of data stored on Board computer systems must be protected by access controls to ensure that only authorized staff and subcontractor users have access and that non-repudiation and digital signatures are verifiable. The chosen method of establishing these services and the Server will be via **Verisign Security Certificates implementation** on the Exchange Messaging Server. The Verisign Certificate Licensing will protect all email transmissions and enable local users to reset their passwords when needed via the Internet.

Access rights to and the sharing of designated Group Folders via IT Work Request shall be restricted to only those Users designated by their Administrative/Supervisory personnel. The capabilities and "rights" that are appropriate to each staff and subcontractor user's job duties and those Directories shall be established accordingly with Supervisory; Administrative/Executive Staff.

Customer Resumes and personal data **MUST** be protected with local security measures i.e.; password protections and IT Security measures and remain confidential at all times.

1) Network Security Maintenance & Modifications - IT responsibilities

The IT Administrator shall be responsible for the administration of access controls to all Board computer systems. The IT Administrator will process additions, deletions, and changes upon receipt of a written request from the end user's supervisor and following receipt of it's enclosed signature page. Deletions may be processed by an oral request prior to reception of the written request so as to prevent user access to resources immediately upon leaving employment with Board or Subcontractor.

The IT Administrator will maintain a list of administrative access codes and passwords for Servers and keep this list in a secure area. The IT Administrator does not serve as a Password Reminder Service and IT Security provisions recommend against this practice. Where password problems occur the IT Administrator resets User Password generically in the Servers Active Directory and grants Users access and permissions to change and reset to their chosen Password preference.

When Job Rotation occurs from one subcontractor to another within the Boards system they should not be reported as "terminations" for Email editing. (The consequences = the deletion of the User and all previous email settings/records)

2) User Security Responsibilities for Staff and Subcontractors

Each staff and subcontractor users:

- Shall be responsible for all computer transactions that are made with his/her User ID and password.
- Shall not disclose passwords to others. Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords should not be recorded where they may be easily obtained.
- Should use passwords that will not be easily guessed. Don't use a dictionary; they are vulnerable to password-cracking devices. Recommend use of alphanumeric characters with no less than 8 characters and no more than 14 characters Total.
- Should log out (or lock the system (W2K Users only) when leaving a workstation for an extended period.
- Work Requests submitted to IT Network Administrator establishing network resources, establishment of Groups and sharing need to identify level of "User Rights" authorized to be established to maintain the confidentiality and security of the resources.

3) Supervisory Personnel Responsibility – Timely Notice of Changes

Managers and supervisors must notify the IT Administrator promptly whenever a staff and subcontractor user leaves the Board or transfers to another department so that his/her access can be revoked or edited.

4) Human Resource Type Changes – Name Change, Transfer, Terminations

Personnel Changes i.e.; associate transfers, new hires, name changes, and terminations must be reported to IT as soon as possible so Network can accommodate the users needs and remain within the License limitations for access to network services, maintain proper security, and ensure directory listings are as current as possible for all staff and subcontractors.

G. Confidential Information – Protecting Privileged Data

No person(s) shall disclose or use for his/her benefit, or the benefit of any person, corporation, or other entity, any computer file/data concerning confidential information provided by program customers, or coworkers or the Board. Access or use for non-related purposes is a serious offense that will lead to disciplinary action, up to and including actions that may seek termination from employment by offender. For the purpose of enabling the proper disposal of expired confidential records and to prevent privileged confidential information being retrieved from normal trash disposal, all such authorized disposals must be done with the Paper Shredder. High-powered paper shredders are available in all MI Works Customer Centers

H. Physical Security & Redundant Backup Plans for IT Equipment

1) IT Administrator – Develop & Implement Multiple Redundancy & Security

- It is Board policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards and that redundant backup resources are available on site and copies maintained offsite in the event of damage, theft, vandalism or other catastrophic events. This has been planned and accomplished via Digital Data Tape Drive Rotation and RAID technology on the Servers that are hot swappable in case of failure between 3 and 6 drives remain available with identical data on each server.
- Design Plan Topology Manuals and project records remain on file with the IT Administrator and with the Engineering Vendor in case a Emergency Catastrophic event were to occur that required a rebuilding of the current system and a database of equipment inventory has been recorded and is backed up to the server and is kept off-site via tape and data file.
- In addition, we have designed into our plan the implementation of Critical Client working files and settings from one's workstation to local Servers in a manner that is programmed to run on a timed schedule without the Staff person having to think about it. This service has been successfully tested fully in the Board office and is planned for full Network implementation during PY 2002/3.
- The Chosen Customer Use Security Systems Lockout is "Full Armor" Software. Locks PC's and Prevents User change to system settings in the registry, users cannot access areas to create damage intentionally or by accident. This is the same system used in many major retail establishments to prevent user tampering and has worked perfectly with Talent Bank use the past 4.5 years. Newer versions with Network customization may be used in other Public PC's based upon its Success.

2) Staff and subcontractor users Physical Security & Redundancy Plans

- Diskettes with privileged customer data and Program Application CD's with their License Key Codes should be stored out of sight when not in use to prevent theft. If they contain highly sensitive or confidential data, they must be locked up. They also should be kept away from environmental hazards such as heat, direct sunlight, moisture and magnetic fields.

- Critical computer equipment, e.g., file servers, must be protected by an uninterruptible power supply (UPS). Other computer equipment are to be protected by a *surge suppressor that is provided by the Board. Important to understand that Surges cannot stop a direct lightening strike on a building though. Note: The amount of static electrical charge needed to damage or destroy PC motherboard and/or memory chips is actually below what a human being can feel in common household static. It's important to realize that it requires very little electrical fluctuation to cause damage and is precisely why systems are setup so they do not share off circuits of any high-powered electrical components.

- Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided. During severe weather (electrical storms) networked printers and most IT equipment should be powered down and unplugged from the wall receptacle temporarily. Systems should be taken offline if power brownouts are occurring, one way to know is the local UPS systems connected to the Serves monitor power flow and if it reaches extremes it will sound an alarm. Notify IT Department as soon as possible and services need to be done off-line until proper current is restored.

- Since the IT Administrator is responsible for coordinating all IT equipment installations, disconnections, modifications, inventory control and relocations, staff and subcontractor users are not to perform these activities without review, coordination and approval of the IT Administrator. This does not apply to temporary moves of portable computers for which an initial connection has been set up by IT. It's imperative that the movement of any IT equipment be requested in writing FIRST so that the Boards Inventory database is current and in case a State Monitor randomly chooses to audit.

- Staff and subcontractor users shall not take shared portable equipment such as laptop computers out of their assigned workplace environment without the informed consent of their department manager. Informed consent means that the manager knows what equipment is leaving, what data is on it, and for what purpose it will be used and that it's secure from theft during transport, i.e.; out of view within ones automobile to prevent smash and grab threats.

- Staff and subcontractor users should exercise care to safeguard the valuable electronic equipment assigned to them. Staff and subcontractor users who neglect this duty may be accountable for any loss or damage that may result. In the case of stolen equipment a Police Report must be generated and forwarded to the IT Administrator for reporting to the State MDCD as required by the Board's Procurement Guidelines and replacement components may be procured.

3) Supervision of Users – Mission Related Customer Use & Accountability

- It is understood that some of our IT Resources are established to service customers in a "Self Service" environment in our Customer Centers to maximize the availability of services to our Customers and their potential in meeting their goals in obtaining services that will advance their Career and Job Search Goals. While this is a trust relationship designed to maximize our Customers potential there are areas of abuse that have and can occur. Where audits of our IT logs and/or personal observation of Customer use detect abuse of these services then restrictions must be implemented for that Customer, especially where they have ignored our requests or transferred their access to another Customer Center.

- While we want to always maximize our resources to the benefit of our **MI Works!** Customers--Surfing the Web for extended periods using our "Self Service" resources for their Personal Use that isn't mission related is not a proper use of our services and Facilitating Staff must inform the Customer accordingly. Where a Customer has ignored these requests then they need to have restricted supervised access only. We simply lack the resources to become a Web Café for the general public and their personal use of those resources. With the increase of customer traffic in a slowing economy more demand will likely result for use of those systems and restrict our T1 Bandwidth.

Precautionary Note - Special Circumstances on Use/Supervision/License Compliance

Restricting Public User Access. ***(Common sense and reasonable judgment should be exercised)***

While we want to be open and trust the customers use, there are those that may violate that trust and in an unsupervised room could create substantial damage to our network systems or others, especially someone desiring the use of a public PC to distribute viruses or create Denial of Service or SYN attacks. They can use this type of technique to cripple or damage IT Services. The Network Card on every PC has a traceable address on it that will leave a trail back to our Proxy Services and the MAC Address on the PC that was used, however it doesn't identify who was the user. It is the recommendation of IT Services & Standard Networking Protocol that all Customer Users activity be logged for each Customer PC throughout the day for proper accountability

Copyright & License Violations: "Dogbite Rule" and Board Recovery Rights

The Board provides all IT Equipment/Services in good faith for use in delivery of services and Trusts all users to abide by "Use Policies" and Statutes contained herein. Software Piracy laws enforce the "Dog Bite Rule" which means litigants pursue the owner of said equipment, "The Board", not the user when violations are reported. In this relationship of Trust - - The Board ask that these conditions be honored to the benefit of all. However, the Board reserves the right to remedy any such abuses. The Software Piracy Act and what is known as the "Dog Bite Rule" has provisions allowing the Owner (Macomb/St.Clair Workforce Development Board) to recover costs for any damages or penalties imposed upon it through those users that violate the provisions contained herein. (IT Admin)

IT Information Security Policy

I. Copyrights and license agreements

It is Macomb/St. Clair Workforce Development Board's (MSCWDB) policy to comply with all laws regarding intellectual property. Staff and subcontractor users using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by the Board and/or legal action by the copyright owner.

1) Legal reference

MSCWDB and its staff and subcontractor users are legally bound to comply with the Federal Copyright Act (Title 17 of the U. S. Code) and all proprietary software license agreements. Noncompliance can expose MSCWDB and the responsible staff and subcontractor users(s) to civil and/or criminal penalties.

2) Scope

This directive applies to all software/hardware that is owned by MSCWDB, licensed to MSCWDB, or developed using MSCWDB resources by staff and subcontractor users or vendors.

3) IT responsibilities - Re: Copyrights/Licenses - The IT Administrator will:

- Maintain records of software licenses owned by MSCWDB.
- Periodically (at least annually) scan Board computers to verify that only authorized software is installed.
- Coordinate an Annual Audit with the IT Technician to Objectively scan user PC's for unauthorized software applications and services and to conduct remote desktop administrative review of Network user systems and event log's.

4) Staff and subcontractor users responsibilities - Copyrights/Licenses

- Are prohibited from installing software unless authorized by MSCWDB IT. Only software that is licensed to or owned by MSCWDB is to be installed on MSCWDB computers. Any Staff or Subcontractors that request third party software installations must provide receipts of purchase and license certification documents that identify conditions for use. Receipts for purchase and license that may have been obtained for one's home PC or Subcontractor machines for their organization do not legally extend to equipment of the Board and are prohibited unless documented proof authorizing license extension to our systems is provided from the Owner of said License. Bringing in bundled software from one's home or a friend/relative to install is not permitted and considered illegal and can subject the Board to civil/criminal penalties.
- Pre-installed OEM Software that came licensed and resident to that OEM PC cannot be legally transferred.
- Copy software unless authorized by MSCWDB IT.
- Download software unless authorized by MSCWDB IT.
- Install "Freeware" without review and approval by MSCWDB IT. Those staff that desire use of any identified "Freeware" software then a written source confirming it, as "Freeware" must be emailed, faxed, or available for confirmation via the Internet as "Freeware" and IT must review and test it out first for compatibility.
- Where supplemental software purchases/installations may be desired they need to go through a review and approval process with the MSCWDB IT as determined by the Board. This process can determine any potential conflicts and determine the type and volume of license to purchase so as to maximize budget funds and resources. Significant cost savings can result to the Board by examining volume of installation and number of locations/users.

5) Civil penalties - Violations

Violations of copyright law expose the Board and the responsible staff and subcontractor users(s) to the following civil penalties:

- Liability for damages suffered by the copyright owner
- Profits that are attributable to the copying
- Fines up to $100,000 for each illegal copy

6) Criminal penalties - Violations

Violations of copyright law that are committed "willfully and for purposes of commercial advantage or private financial gain (Title 18 Section 2319(b))," expose the Board and the staff and subcontractor users(s) responsible to the following criminal penalties:

- **Fines up to $250,000 for each illegal copy**
- **Jail terms of up to five years**

Acknowledgment of Information Security Policy

This form is used to acknowledge receipt of, and compliance with, the Macomb/St. Clair Workforce Development Board, Inc. Information Security Policy.

Complete the following steps:

1. **Read the Information Security Policy.**
2. **Sign and date in the spaces provided below.**
3. **Return this page only to the Information Technology Administrator.**

By signing below, I agree to the following terms:

i. **I have received and read a copy of the "Information Security Policy" and understand the same;**

ii. **I understand and agree that any computers, software, and storage media provided to me by the Board contains proprietary and confidential information about Macomb/St. Clair Workforce Development Board, Inc. and its customers or its vendors, and that this is and remains the property of the Board at all times;**

iii. **I agree that I shall not copy, duplicate (except for backup purposes as part of my job here at Macomb/St. Clair Workforce Development Board, Inc.), otherwise disclose, or allow anyone else to copy or duplicate any of this information or software;**

iv. **I agree that, if I leave Macomb/St. Clair Workforce Development Board, Inc. for any reason, I shall immediately return to the Board the original and copies of any and all software, computer materials, or computer equipment that I may have received from the Board that is either in my possession or otherwise directly or indirectly under my control.**

v. DISCLAIMER STATEMENT: For Board employee's, subcontractor staff, and customers using the Internet –

   1. No Warranties of any kind, expressed or implied, when transacting business over the Internet. This includes loss of data resulting in delays, non-deliveries, misdeliveries, or service interruptions caused anywhere in the Network. While it is the ongoing goal of IT to prevent network downtime as much as possible there are times that errors occur within the infrastructure that require downtime to correct an issue or that a component may fail and require acquisition and replacement or third party troubleshooting.
   2. Use of any information obtained via the Internet is at the User's own risk, and no warranty is made as to accuracy or quality of the information obtained.

Agency Employed By: _____

Worksite Location: _____ **Department:** _____

Staff and/or Subcontractor users name: _____

Staff and/or Subcontractor users Job Title: _____

Staff and/or Subcontractor users signature: _____

Date: _____

Macomb/St.Clair Workforce Development Bd., Inc.

IT HelpDesk Triage Policy

*The contact and resolution times given below are the IT department's general guidelines under normal circumstances. During extraordinary situations, such as a natural disaster, prolonged power outage, or other catastrophic events, contact and resolution times may be longer.

Priority	Issue	Contact	Resolution
#1	**Event of the Highest Importance -** Mission-critical systems with a direct impact on the organization LAN/WAN (Examples: widespread network outage, telecom system, Server Rack Integrity & Backup Resources, Natural Disaster, Fire, Theft, Vandalism, Security Breach, Virus Contamination, etc.)	**IMMEDIATE** Problematic Diagnostic Tools to identify Event source(s). Test & ID Source for Course of Action.	**IMMEDIATE** Consultation w/Engineer Support or Telecom T1 Carrier(s) to identify/resolve issues/events for a return to "Normal" ASAP.
#2	**Event affecting Core IT Services at a MI Works Customer Center preventing delivery of local mission critical services.** (e.g.; Local Server failure, T1 Loss, TCP/IP Internet Services or Hubs/Router Failure. Local Traumatic Event/Disaster, Fire, Theft, Vandalism,etc..)	**IMMEDIATE** Problematic Diagnostics to identify Event source(s).	
#3	**Event is preventing the affected user(s) from working** (Examples: failed hard drive, broken monitor, continuous OS lockups, etc.) Individual User inconvenience. All Centers have redundant PC's, Printers for emergency use as backup and we use Dynamic IP for access from any PC within our Network.	***As soon as possible (ASAP)!** Via Email, Fax, Phone.	***Same Day or NBD Preferred.**
#4	**Scheduled Projects** (Examples: new workstation installation, new equipment, new hardware/software installation, peripherals)	***Same Day Response** Via Email, Fax, Phone.	1 – 4 Days
#5	**Event can be permanently or temporarily solved with a workaround** (Examples: malfunctioning printer, fax, PDA synchronization problem, PC sound problem, etc., e.g..; redundant network shared resources)	***Same Day Response** Via Email, Fax, Phone.	5 Days
#6	**Nonessential scheduled work** (Examples: office moves, equipment moves & loaners, scheduled events, supplemental enhancements) Incidental upgrades, patches, customization services, hands-on or remote training services support that improve usability, productivity and IT Skills Proficiency of Board and Subcontractor Staff thereby improving IT Services Delivery overall. Remote "PUSH/PULL" desktop modifications/maintenance services overnight through the Network Domain Servers to W2K Network Services.	**As time Permits** when convenient could be immediate or matter of days/weeks. Via Email, Fax, Phone- or when performing other services.	**Coordinated with recurring tasks.** After all other essentials are resolved first. Ongoing Services.